Code of Practice for Cloud Service Providers

This Code of Practice for Cloud Service Providers ('Code') from the Cloud Industry Forum ('CIF') is for organizations offering to customers remotely hosted IT services of any type. These services include, but are not limited to, multi-tenanted services accessed via the Internet.

Organizations claiming compliance with the Code shall conduct an annual Self-Certification and confirm the successful results of this Certification to the CIF in order to receive authorization to use the Certification Mark (the 'logo') for the following year. The Self-Certification claims will be listed on the CIF website **(www.cloudindustryforum.org)** and hyperlinked from the logo displayed on the participant site. Optionally, an organization may opt for Independent Certification performed by a Certification body approved by the CIF, and will then receive authorization to use the 'Independent Certification Mark' for the following year. The CIF will spot check and randomly audit Self-Certifications as well as investigate any formal complaint of non-compliance against an organization claiming compliance with the Code. In the event of finding a false declaration or material non¬-conformity, at the sole discretion of the CIF, the authorization to use the Certification Mark shall be immediately suspended, pending resolution, or terminated, and this action shall be documented on the CIF website, and may be reported publicly such as via press releases.

A. Transparency

The first and most important pillar of the Code is to ensure a reasonable and consistent level of transparency about businesses and their operational practices throughout the Cloud Industry. The Code does not specify best practice in Cloud Computing except with respect to transparency.

Organizations complying with the Code shall conduct themselves in an open and transparent manner which facilitates rational decision-making and management by purchasers of their services. The Code, however, does not set out to and will not make decisions for purchasers, but will simply help to ensure that essential information is available to make decisions.

There are two categories of information which shall be disclosed: (1) information for public disclosure; and (2) information for contracting disclosure, which may either be publicly disclosed or commercial-in-confidence subject to non-disclosure terms.

A.1. Information for Public Disclosure

Information for public disclosure should be readily available on the organization's website in the format and location specified by the CIF, with a hyperlink to the CIF website. The CIF website will also have available the relevant information which was provided at the time of the Certification Application. The information on the organization's website should be kept up-to-date (within 4 weeks of changes occurring), whereas the CIF website will be updated only as part of the annual Certification Application process.

Optional categories of information (designated below by 'Optional'), if publicly disclosed, shall include all of the types of information shown for each category. Any optional categories of information which are not publicly disclosed shall be disclosed as part of "Information for Contracting". (Disclosure of Industry Association Memberships is optional in both cases.)

A.1.1. Compliance with Code

- Statement that the organization commits to complying with the Code for the scope covered by the Application (see A.1.3).
- Link to the organization's website page where publicly disclosed information is available, including a statement of commitment to complying with the Code. [Note: this shall be as specified in IP11 Format for Public Disclosure.]

A.1.2. Corporate Identity and Responsibilities

[Note: The information in this section is for the legal entity which contracts with the purchaser of cloud services covered by the Code. It should not be a separate marketing or operational entity.]

- Corporate name
- Legal status, date of formation, location of registration, and registration number
- Ownership (major shareholders)
- Members of board of directors (or equivalent body)
- Executive management (CEO and CFO or equivalents)
- Corporate fixed address [not a post office box]

A.1.3. Scope Covered by the Code

[Note: The on-line Registration allows, and on-line Application process requires, the specification of the scope of services covered by the code by means of multiple selection drop-downs, to facilitate customer searches. However, the free-format statement of scope in this section is the definitive one, and typically will include product or service names.]

- Scope of services [free format]
- Geographical scope [based on drop-downs]
- Countries with local sales and/or support
- Countries where customer data may be held or processed
- Statement about whether the customer can restrict the countries where customer data may be held or processed

A.1.4. Public Branding

[Note: The information in this section is only for the scope of services covered by the Code.]

- Alternative trading name(s) if different [Any alternative marketing or trading ('doing business as') names]
- Website address(es) [Websites used to market the services covered by the Code (whether owned by the contracting legal entity or not) All of these websites must provide the information for public disclosure required by the Code.]

A.1.5. Third-Party Coverage Transparency

- Statement about the extent to which the organization accepts indirect responsibility for the organization's suppliers. [This covers e.g. the situation of the organization's suppliers going out of business.] For example: for the technical failure of vendors in the supply chain such as collocation where services are taken off-line
- Statement about the extent to which the organization's suppliers accept indirect responsibility to the organization's customers. [This covers e.g. the situation of the organization itself going out of business.] For example: if the organization aggregates third-party services that are on-sold to the organization's customers, do the third-party supplier contracts offer reciprocal terms and protections e.g. liability, service level resolution, data protection
- Statement about extent to which the organization accepts indirect responsibility to customers of customers. [This covers e.g. the situation of the organization's direct customers going out of business.] For example: to customers of customers for access to data if the direct customer goes into administration or liquidation

A.1.6. Security Control Transparency with the Cloud Security Alliance

Statement about whether the organization has completed the Consensus Assessments Initiative Questionnaire from the Cloud Security Alliance (https://cloudsecurityalliance.org/cai.html), which "provides a set of questions which a cloud consumer and cloud auditor may wish to ask of a cloud provider" to provide "security control transparency"

A.1.7. Other Extended Commitments to Code of Practice Principles

- Statement about whether the organization commits to any additional transparency, capability, or accountability requirements in addition to those contained directly in this Code of Practice.

A.1.8. Technological Commitments (Optional)

- Statement about whether there are any specific technologies, standards, or inter-operabilities which the organization commits to supporting. (There is no requirement to support any specific technologies etc, but it should be clearly stated whether there are any such commitments. Standards may be formal or under development, as long as they are specifically referenceable.)

  Reference to where relevant information about the technology, standard, or interoperability can be obtained.

A.1.9. Existing Certifications (Optional)

- List of any existing relevant certifications, e.g. ISO 9001, ISO/IEC 27001, PCI DSS, SAS 70 and SSAE 16/ISAE 3402
- Statement of scope of business covered by Certification, and how it corresponds to scope of Code
  By whom Certification was performed, if independently certified

A.1.10. Industry Association Memberships (Optional)

- List of any industry associations in which the organization has a membership

  Reference to the organization's website

A.2. Information for Contracting Disclosure

This information is for disclosure in connection with proposals and contracts. Where contracts are individually negotiated and signed, this information will typically be subject to non-disclosure terms. When contracts are non-negotiable, and typically signed on-line, then this information shall be made available prior to contract signing. This could be by means of disclosure on the organization's web site, by hyperlinked reference in the organization's contractual terms and conditions, or in any other way. To the extent that a customer will rely on any of this information, or on publicly-disclosed information, it should be made part of contractual terms and conditions.

A.2.1. Commercial Terms

- Pricing policy (basis of charging with fully-declared costs)
- Payment terms
- Contract lengths and options for discount for longer commitment
- Termination basis, terms and conditions
- Renewal and amendment terms and process

A.2.2. Personnel Profile

- Number of full-time personnel by band

  (1-10, 11-50, 51-200, 201-1000, 1000+)
- Number of staff based outside of the defined territory by band

  (1-10, 11-50, 51-200, 201-1000, 1000+)
- Employee vetting procedures undertaken

A.2.3. Customer Migration Paths at Contract Termination

- Declaration of any commercial restrictions
- Technological implications (e.g. is there technological lock-in that prevents migration to other suppliers or in-house)
- Format of data provision and transfer
- Cost implications (e.g. are there any costs associated with recovering data, or for purchasing replacement licenses)

A.2.4. Customer Migration Paths during Contract Execution

- Implications in the event of the organization itself, or the organization's suppliers, changing their provision of services, or ceasing business (e.g. is there technological lock-in with a specific supplier)
- Ability to retrieve data in such situations

A.2.5. Licensing Provisions

- Who is responsible for any software/IP licensing, and any costs involved which are not covered within the cost of the services being provided
- Whether there are any licensing implications in addition to cost, including in particular whether *GPL is used potentially requiring publication of all code whether original code modified or not

A.2.6. Provisions for Information Security

- Overview of measures in place to provide for information security in general

A.2.7. Data Protection Provisions

- Countries and locations where data will/may be held during the term of the contract, and where processing will/may take place including for backup purposes
- Data protection legislation which will be relevant to the contract
- Overview of measures to ensure compliance with relevant legislation and to ensure data privacy

A.2.8. Provisions for Service Continuity

- Overview of measures, including redundancy, to provide for service continuity including protection against data loss

A.2.9. Provisions for Audit

- Ability to arrange independent audits of the provider organization for various purposes, e.g. security, license compliance and CIF audits

A.2.10. Service Dependencies

- Clarification of any sub-contracting or co-location relationships (names may or may not be given)
- Implications of service dependencies for service levels
- Compliance with data protection requirements
- Continuity of operations

A.2.11. Complaints and Escalation Procedures

- Complaint procedures
- Escalation procedures and named individuals for escalation

B. Capability

A second pillar of the Code is 'capability', by which is meant the ability of an organization to perform essential management functions, as demonstrated by having in place auditable documented management systems. 'Capability' is fundamentally different from 'transparency', although there should be a reasonable degree of transparency about capability. For this reason there are a number of requirements in the 'transparency' section about capabilities, but those disclosure requirements are not the same as actually having documented management systems in place. Note that there is no disclosure requirement for the details of the management systems specified by this pillar of the Code. CIF itself may audit these management systems, but the organization does not need to say anything publicly about these systems, except to the extent that they are covered by general disclosure requirements in section A above.

A documented management system shall include, at a minimum, (a) written policies and procedures, (b) specific individuals assigned with relevant responsibilities, and (c) appropriate training and awareness programs. These requirements are similar to, but less onerous than, full management system standards like ISO 9001 (quality management), ISO/IEC 27001 (security management), and ISO/IEC 20000-1 (service management).

The specific areas for which documented management systems are required for the Code are:

- Information Security Management (including Data Protection)
- Service Continuity Management
- Service Level Management
- Supplier Management
- Software License Management (including License Compliance)
- Complaint Handling
- Environmental Impact Management

The first four of these are areas specifically covered by ITIL® V3, for reference by organizations seeking general guidance. The last three are not explicitly covered in ITIL V3 at the same level, but are considered critical to success for organizations operating in the Cloud Industry. (ITIL® is a registeredr trademark of the Cabinet Office)

The extent of documented systems needed to meet the requirements of the Code will vary depending on organizational size. For a large multi-national organization, there will likely be extensive policy and procedure documentation. For a small two-person business, the documentation requirements will be limited, but a minimum level of documentation will still be needed. For example, the documented management system for complaint handling for a small two-person company could be a simple statement that all complaints will be handled by Person A, and reviewed by Person B. For a larger organization, a more extensive process would usually be required, with a provision for appeals. Information security management would typically require more extensive documentation, even in smaller organizations, and include for example a list of the regular information security control checks and reviews which are to be performed.

Organizations complying with the Code may wish to consider certification against relevant standards for the requirements of this section, such as ISO 9001:2000 or ISO/IEC 27001:2005. For smaller organizations and for organizations which do not consider such certifications appropriate, the CIF may in the future develop prototype management system documentation for the required areas.

C. Accountability

Organizations which assert that they are complying with the Code shall be accountable for their compliance with the Code and for their behavior with customers.

C.1 Accountability for Compliance with the Code

The CIF will revoke the Certification of any organization deemed not to be complying with the Code. Furthermore, this revocation will be publicized on the CIF website, and potentially be reported publicly such as via press releases.

Potential non-compliance with the Code may be brought to the attention of the CIF in two separate ways: (a) as the result of customer or whistle-blower complaints to the CIF; and (b) as a result of spot check and random audits conducted by the CIF itself, or its appointed agents. Customer or whistle-blower complaints may also result in such audits being conducted.

To enable auditing by CIF of compliance with the Code, an organization shall maintain auditable records to demonstrate its compliance for a minimum of 14 months, extended during any period while an active CIF investigation or audit has been notified to the organization. The dated auditable records to be maintained shall include:

- Copies of information for public disclosure as shown on the organization's website(s) and updated from time to time
- Copies of information for contracting disclosure, whether as shown on the organization's website(s) and updated from time to time, or as separately disclosed to potential customers, identifying those potential customers

C.2 Accountability for Behavior with Customers

Organizations complying with the Code shall make two provisions to provide accountability for behavior with customers:

- Provision of formal procedures for complaint resolution within the organization itself
- Willingness to agree to binding arbitration in local courts for the settlement of disputes. The CIF can provide expert witnesses to facilitate such arbitration.

These accountability requirements are separate from any which are created by legislation or regulation, such as accountability to adhere to the principles and guidance of the Advertising Standards Agency in the UK in regard to web-based content and advertising.

Contact Us

Mail: The Cloud Industry Forum, Sword House, Totteridge Road, High Wycombe, HP13 6DG

www.cloudindustryforum.org

https://selfcert.cloudindustryforum.org

Email: info@cloudindustryforum.org / servicedesk@apmgroupltd.com

Telephone: +44 (0)844 583 2521 / +44 (0)1494 459 559